2.3. Análisis IoT

Utilizando la M. Virtual que puedes descargar de la sección Archivos de este equipo y cuyo nombre es Raspbian, trata de responder a todas las cuestiones que te planteamos en el documento adjunto. Tienes mucha información adicional que puede ayudarte a contestar y resolver este reto en la presentación 'IoT.pptx' de la unidad 07 del curso 'Análisis Forense Informático' en https://cursos.iesalisal.es

Contenido

Preparación **2**
Entorno de trabajo 2
Pasos a seguir 2
Búsqueda de la IP de la máquina objetivo **2**
Conocer la IP de nuestra máquina y los rangos de IP de la red 2
Descubrir los hosts activos en la red 2
Escaneo de puertos **3**
Escaneo de puertos de la máquina objetivo usando nmap 3
Desafío web sencillo **4**
Navegación manual por la web 4
Análisis del código fuente con Mozilla Firefox 4
Ataque de contraseñas básico con contraseñas por defecto **5**
Búsqueda de log in default 5
Acceder vía SSH 5
Escalado de provilegios **6**
Comprobación de permisos 6
Intento de acceder a archivos restringidos 6
Un nuevo ataque de contraseñas 7
Crear un nuevo usuario para poder continuar accediendo 7

Preparación

Entorno de trabajo

- **Máquina atacante**: Kali Linux
- **Máquina objetivo**: Debian

Pasos a seguir

Configuración de las máquinas:

- Abrir Hyper-V
- Iniciar las dos máquinas
- Conectarse a la máquina Kali
- Una vez que cargue el sistema introduce las siguientes credenciales: usuario: *kali*; contraseña: *kali*

Búsqueda de la IP de la máquina objetivo

Conocer la IP de nuestra máquina y los rangos de IP de la red

- Usa la herramienta *ifconfig* en Kali para saber el rango de IPs de la red, y nuestra propia IP
- Para ello abre la consola y ejecuta el siguiente comando:
    - *ifconfig*

- Ejemplo de resultado de la ejecución:

Descubrir los hosts activos en la red

- Usando *nmap* podemos conocer qué máquinas están activas en nuestra red (192.168.0.0/24)
- Para ello abre la consola y ejecuta el siguiente comando:
    - *nmap -sn <ip_red>/<mascara_red>*

- Ejemplo de resultado de la ejecución:

```
┌──(root💀kali)-[~]
└─# nmap -sn 192.168.0.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-19 10:38 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0026s latency).
MAC Address: 00:15:5D:00:04:00 (Microsoft)
Nmap scan report for 192.168.0.70
Host is up (0.0041s latency).
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Nmap scan report for 192.168.0.60
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.13 seconds
```

- En este caso, la IP de la máquina objetivo es 192.168.0.70

Escaneo de puertos

Escaneo de puertos de la máquina objetivo usando nmap

- Usa *nmap* para escanear los puertos de la máquina objetivo y poder localizar posibles puntos de entrada al sistema
- Para ello ejecuta en la consola el siguiente comando:
  - *nmap -A -Pn -p- 192.168.0.70*

- En la siguiente imagen se muestra el resultado de la salida:

```
┌──(root💀kali)-[~]
└─# nmap -A -Pn -p- 192.168.0.70
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-19 10:32 EDT
Nmap scan report for 192.168.0.70
Host is up (0.0045s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 c0:64:19:ca:b6:ef:de:99:55:c4:ae:ae:2b:4a:32:10 (RSA)
|   256 13:d4:ef:79:d5:53:00:05:59:c0:90:fe:1a:e5:b6:ea (ECDSA)
|_  256 54:d3:a3:4d:12:51:f2:52:39:89:ed:33:a4:57:6a:08 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: H4ck m3 1f y0u c4n!
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   4.47 ms 192.168.0.70

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 177.54 seconds
```

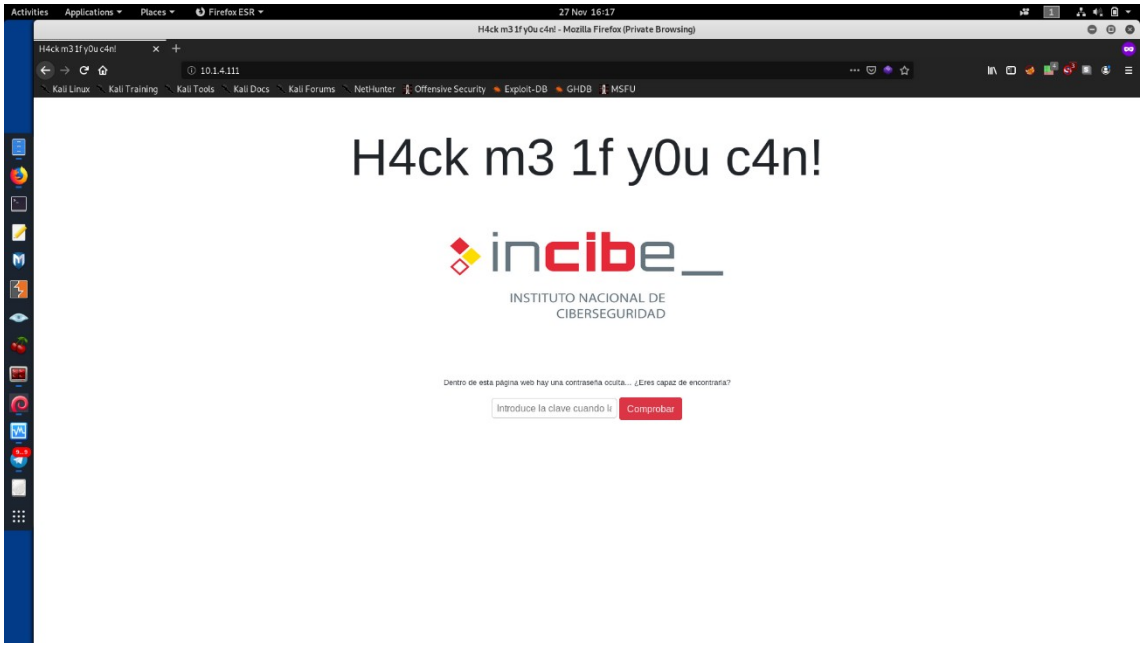
- De este resultado se pueden obtener las siguientes conclusiones:
  - **Sistema Operativo**: Debian Linux 10
  - **Servidor web**: Apache
  - **Puertos abiertos**: 80/TCP (HTTP) y 22/TCP (SSH)
  - Versión del kernel Linux

- En el caso de que *robots.txt* no estuviera, se podría hacer uso de herramientas como *DIRB* o *GoBuster* que, utilizando diccionarios de nombres de directorios comunes, listan los directorios existentes en el servidor web

Desafío web sencillo

Navegación manual por la web

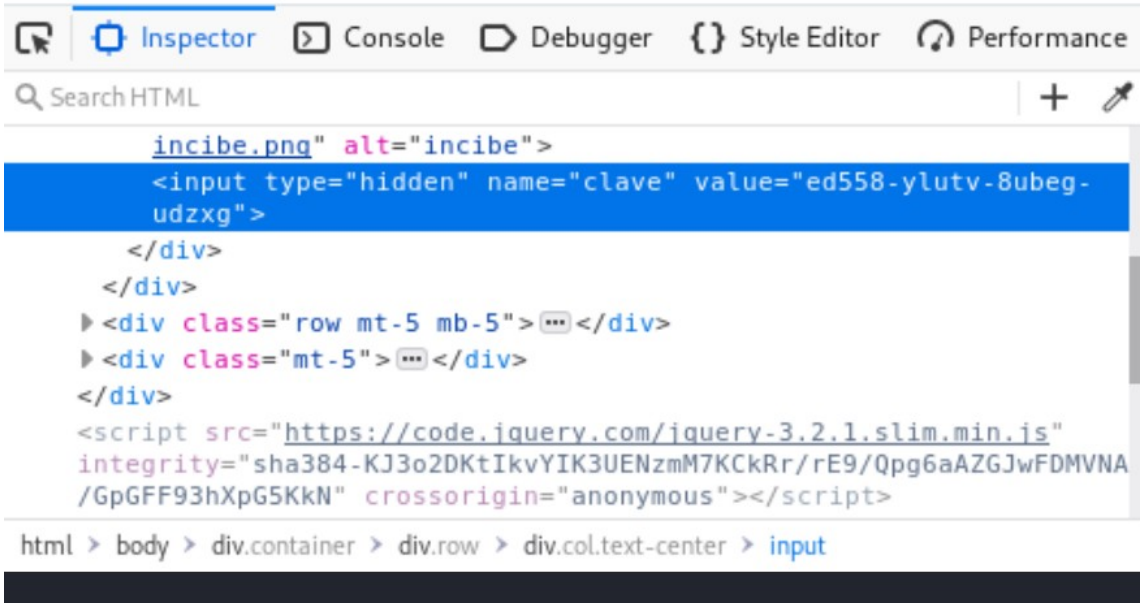
- Dado que el puerto 80 está abierto, haciendo uso de un navegador, accede a la siguiente url para analizar la web:
    - http://192.168.0.70/



- Como podemos observar hay un formulario que nos pide que introduzcamos una clave. Esto es básicamente una CTF super sencilla que muestra una de las posibilidades que nos da el hacking a dispositivos IoT.

Análisis del código fuente con Mozilla Firefox

- **La clave está en el código fuente.** Para encontrarla hay que mirar el código.
- Desde el navegador pulsamos F12 y buscamos entre el código HTML. La clave está en un input oculto.



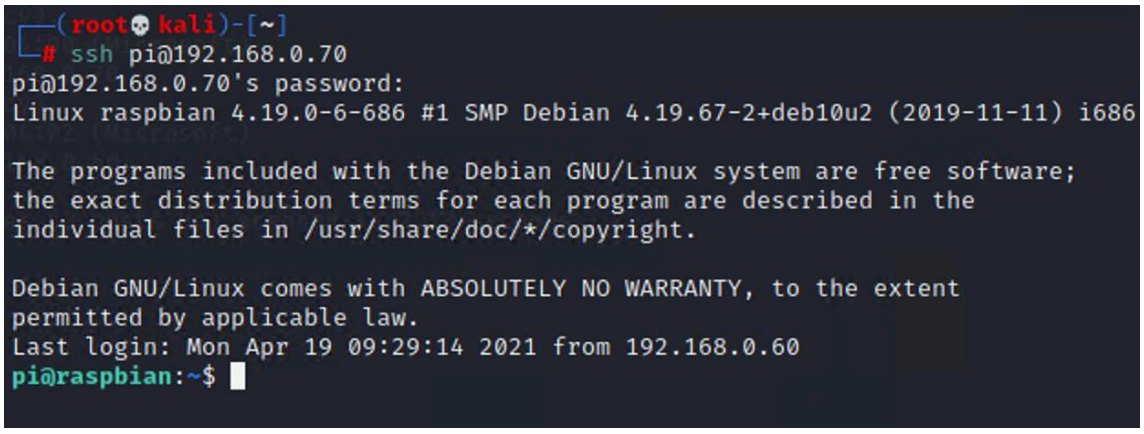
Ataque de contraseñas básico con contraseñas por defecto

Búsqueda de log in default

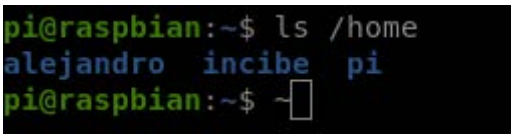
- Raspbian, como muchos otros OS, viene con un usuario ya creado de serie. Este usuario es posible que permanezca presente con la contraseña por defecto en la máquina.
    - La idea es que el alumnado busque si hay un usuario y contraseña preinstalado para Raspbian. Deben encontrar el login *pi* con password *raspberry*.
    - En este caso sí que no están modificados, así que tenemos un acceso garantizado.

Acceder vía SSH

- Sabiendo que la Raspberry tiene un servidor SSH acceder vía:
    - ssh pi@192.168.0.70



- Una vez dentro, se puede ir navegando por los directorios y buscar los archivos y directorios solicitados por el formulario.
- Para hallar el número de usuarios con home bastaría con ejecutar *ls /home*

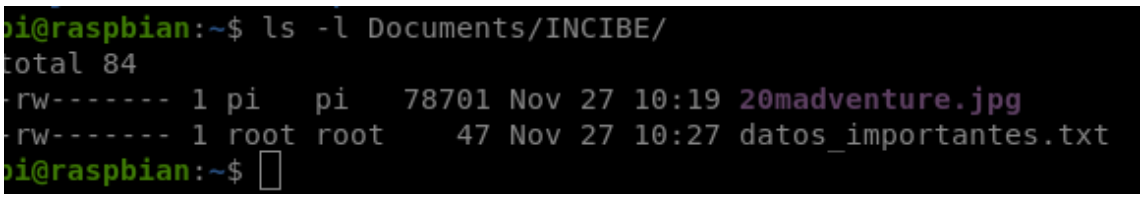


Escalado de provilegios

Comprobación de permisos

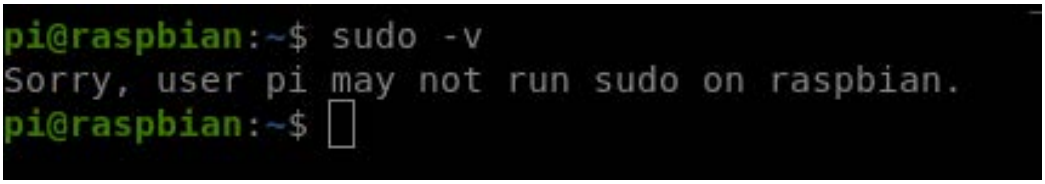
- En caso de que no tengamos seguro con qué usuario estamos logueados podemos usar el comando *whoami*. Nos será relevante en cuanto nos pongamos a intentar acceder con otros usuarios.

- Comprobamos los permisos que tiene el usuario *pi* en *Documents/INCIBE*, utilizando el siguiente comando:
    - *ls -l ~/Documents/INCIBE/*



Intento de acceder a archivos restringidos

- Tras analizar los directorios y archivos acabamos encontrando dos archivos, uno llamado *20madventure.png* y otro llamado *datos_importantes.txt*. Al primero de ellos tenemos acceso porque nuestro usuario es el dueño, pero el otro dispositivo es solo accesible por el usuario *root* y los que estén en la lista *sudores*.
- Con esto en mente sabemos cual es el siguiente paso: buscar la forma de saltarnos esta seguridad adicional.
    - Buscamos si nuestro usuario tiene permisos de acceso a root con:
        - *sudo -v*

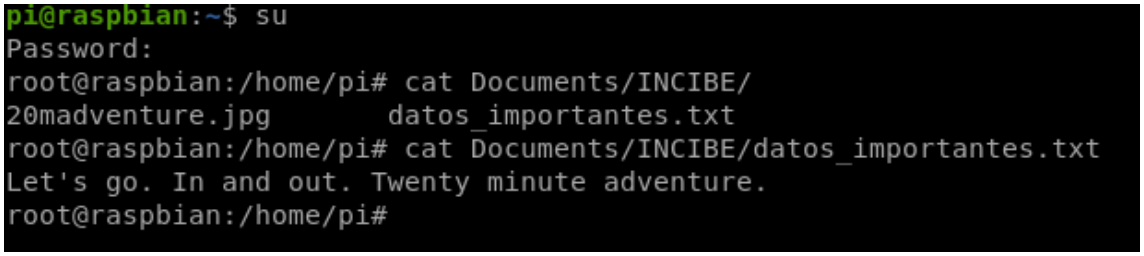


        - En este caso debería fallar, mostrando que no podemos ejecutar *sudo* con este usuario.
    - Tras probar con otros posibles usuarios vemos que no parece posible usar usuarios comunes para obtener permisos de superusuario. En esta situación lo único que nos queda por probar es hacer un log in como root directamente.

Un nuevo ataque de contraseñas

- Siguiendo la pista encontrada en el paso anterior, vamos a hacer lo mismo que hicimos en el primer paso y a buscar contraseñas típicas. Con suerte el usuario root de esta máquina estará tan pobremente configurado como el resto. Para hacer el log in como *root* hay que usar el siguiente comando:
    - *Su*
    - La respuesta es *toor*.

- Tras conseguir crackear al usuario *root* podremos acceder al archivo que hasta ahora no podíamos leer.



Crear un nuevo usuario para poder continuar accediendo

- Una vez hemos podido comprometer al usuario raíz, quizás nos convenga crear un nuevo usuario para seguir accediendo en el futuro a la Raspberry en caso de que nuestra víctima se de cuenta y cambie sus credenciales.
    - Para ello hay que ejecutar el comando *addusr* con la sesión de *root* abierta.
    - Como querremos que nuestro nuevo usuario sea sudoer, tendremos que ejecutar:
        - *usermod -aG sudo <nombre del usuario>*.

      Con este comando acabamos de darnos acceso a las funciones de sudo. Cerramos sesión de *root* con *exit* y ejecutamos:
        - *su - <nombre del usuario>*.